

**Purpose:** This policy describes ILHIE Authority and Participant responsibilities as related to authentication of an Authorized User's identity for the purposes of verification in order to prevent unauthorized users from accessing Protected Health Information available through the ILHIE.

**Policy:** The ILHIE Authority and Participants shall each verify the identity of its respective Authorized Users consistent with National Institute of Standards and Technology ("NIST") Level 3 guidelines. NIST Level 3 authentication should be in accordance with the NIST Special Publication 800-63-2 Electronic Authentication Guideline, as revised from time to time.

- 1.0 Authentication.** The ILHIE Authority and Participants shall each implement user authentication policies and procedures for the purposes of verification of its respective Authorized Users as a prerequisite to permitting an Authorized User to access the ILHIE.
  - 1.1** The ILHIE Authority and Participants shall each designate Authorized Users within their respective organizations that will be authorized to access information available through the ILHIE.
  - 1.2** Each of Participant's Authorized User must be appropriately authenticated by its Participant's System or directly authenticated by the ILHIE System in order to access the ILHIE. The ILHIE Authority will grant Participant Authorized User(s) access to the ILHIE through the Participant's System in reliance upon the Authorized User's authentication through the Participant's System.
  - 1.3** The ILHIE Authority shall verify and authenticate Participant System Administrators in accordance with NIST Level 3 guidelines.
  - 1.4** The ILHIE Authority and each Participant shall verify and authenticate its respective Authorized Users using appropriate identification and authentication procedures in accordance with the NIST Level 3 guidelines.
- 2.0 Password Controls.** The ILHIE Authority and Participants shall each implement and enforce internal policies applicable to its respective Authorized Users governing the use of unique identifiers and passwords.
  - 2.1** All Authorized Users shall be assigned unique identifiers and passwords.
  - 2.2** Consistent with industry and government best practices, the ILHIE Authority and Participants shall each implement Authorized User password procedures including, but not limited to, password strength requirements; re-setting and re-use of passwords; response to failed access attempts including a lock-out mechanism; automatic log-offs; and log-in monitoring to protect against

password guessing. Authorized Users shall be required to keep their user names, passwords and other security measures for connectivity confidential.

**3.0 Information Systems Activity Review.** The ILHIE Authority shall generate audit logs of the ILHIE System in a standardized format such as Audit Trail and Node Authentication (ATNA) to record Authorized User ILHIE System access and activity.

**3.1** Participant shall generate audits logs in a standardized format such as ATNA to record Authorized User ILHIE System access and activity from Participant's System, and upon reasonable request make available to the ILHIE Authority such audit logs for the purpose of matching against the ILHIE audit log. Participant shall review the generated audit logs on a routine basis.

**3.2** The ILHIE Authority and Participants shall implement authentication mechanisms in accordance with the Information Systems Activity Review Policy (Policy #20) to consistently pass along ILHIE Authority compliant authentication information.

**4.0 ILHIE Authority Review.** The ILHIE Authority has the right to review Participant authentication policies and may audit Participants for compliance at any time.

**5.0 Compliance.** Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

**5.1** Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

**Associated Polices and References:**

45 C.F.R §164.312(a); 45 C.F.R §164.312(d)

Breach Notification and Mitigation

Enforcement

Information Systems Activity Review

Sanctions

User Authorization

**Definitions**

Authorized Users

ILHIE Authority

NIST

Participant

Protected Health Information

System Administrator